Express Mail No. EL403199825US
Attorney Docket No. 14102.0002
NON-PROVISIONAL PATENT

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TO ALL WHOM IT MAY CONCERN:

Be it known that I, **Nicolas J. Hammond,** having a post office address and a residence address at 211 East Wesley Road, Atlanta, Georgia 30305-3774, a citizen of the United Kingdom, have invented new and useful improvements in a

METHOD AND APPARATUS FOR AUDITING NETWORK SECURITY

for which the following is a specification.

METHOD AND APPARATUS FOR AUDITING NETWORK SECURITY

CROSS REFERENCE TO RELATED APPLICATIONS

This application is related to copending provisional application Serial No. 60/146,175, filed July 29, 1999, which is incorporated by reference, and claims the benefit of its earlier filing date under 35 USC Section 119(e).

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer network security and, more specifically, to a method and apparatus for auditing computer network security.

2. Description of the Prior Art

As use of large computer networks becomes more prevalent, computer security increases in importance. To reduce networked computer vulnerability, many organizations run periodic security audit scans of their computer systems. Such scans typically involve a dedicated scanning machine that attempts to gain unauthorized access to a computer system via a computer network through a variety of methods. The scanning machine will make numerous attempts to gain access and maintain a record of any security breaches that it detects.

Conventional scanning systems perform scans on command and are frequently dedicated to only a single user. Thus, scans are not performed periodically unless the user remembers to activate the scanning machines. Furthermore, many scanning machines are idle for large periods of time.

Therefore, there is a need for a scanning system that periodically schedules security scans of several users.

SUMMARY OF THE INVENTION

The disadvantages of the prior art are overcome by the present invention which, in one aspect, is an apparatus for auditing security of a computer system. At least one secure application server is in communication with a global computer network. The secure application server is programmed to receive selectively security audit instruction data from the remote computer system via the global computer network. A plurality of scanning machines each are in communication with the global computer network and are programmed to execute selectively a security audit scan of the remote computer system via the global computer network. A central computer, having a memory, is configured as a database server and as a scheduler. The central computer is in communication with the secure application server and the scanning machine. The central computer is programmed to perform the following operations: evaluate a database to determine if a security audit scan is currently scheduled to be run for a user; determine which of the plurality of scanning machines is available to perform a security audit scan; copy scan-related information into a scanning machine determined to be available and instruct the scanning machine to begin scan; and record the results of the scan in the memory.

In another aspect, the invention is a method of auditing security of a computer system in which an instruction to perform a security audit scan on a computer system is received from a user via a global computer network. A scanning machine is instructed to access the remote computer system via the global computer network and thereby perform a security audit scan of the remote computer system. At least one result of the security audit scan is reported to the user once the security audit scan is complete.

In yet another aspect, the invention is a method of auditing computer system security in which a database is accessed to determine when a security audit scan of a computer system is to be executed. Upon determining that a security audit scan of the remote computer system is to be executed, security audit scan data is copied into a scanning system, the scanning system is caused to establish communication with the remote computer system via a global computer network and to execute a security audit scan of the remote computer system via the global computer network. A result of the security audit scan of the global computer network is stored and a message is transmitted to a user of the remote computer system that indicates the result of the security audit scan.

These and other aspects of the invention will become apparent from the following description of the preferred embodiments taken in conjunction with the following drawings. As would be obvious to one skilled in the art, many variations and modifications of the invention may be effected without departing from the spirit and scope of the novel concepts of the disclosure.

BRIEF DESCRIPTION OF THE FIGURES OF THE DRAWINGS

FIG. 1 is a schematic diagram of the devices employed in one embodiment of the invention.

FIG. 2 is a flow chart showing the steps executed in one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

A preferred embodiment of the invention is now described in detail. Referring to the drawings, like numbers indicate like parts throughout the views. As

used in the description herein and throughout the claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise: the meaning of "a," "an," and "the" includes plural reference, the meaning of "in" includes "in" and "on." Also, as used herein, "global computer network" includes the Internet. A "secure application server" could include any digital machine that controls a computer communication and includes security features that inhibit unauthorized access.

As shown in FIG. 1, one embodiment of an apparatus **100** for auditing security of a remote computer system **102** or a remote network **104** is resident at a central site **110**. A central computer **120**, including a computer-readable memory, is configured as a database server and acts as a scheduler. The central computer **120** is in communication with at least one secure application server **130** and a plurality of scanning machines **140**, of the type generally known in the art of computer network security analysis. The secure application server **130** (for example, an Internet Web server) is in communication with a global computer network **106** (such as the Internet) and is programmed to receive selectively security audit instruction data from the remote computer system **102** via the global computer network **106**. A plurality of scanning machines **140a-n** is in communication with the global computer network **106** and each is programmed to execute selectively a security audit scan of the remote computer system **102** via the global computer network **106**. A security audit scan could include, but is not limited to, any combination of the following forms of security assessments generally known to the art of computer network security analysis: security audit scan; security scan; audit; audit scan; remote assessment; vulnerability assessment; vulnerability analysis; and penetration study.

As shown in FIG. 2, one illustrative embodiment of the general procedure executed by the central computer **120** includes assigning **200** the value of zero to an iteration variable and performing a test **202** to determine whether a security audit scan is scheduled for the current period. If a scan is not scheduled, the central

computer **120** performs a test **118** to determine if a user has requested a scan. If a scan is scheduled, or if the user has requested a scan, the central computer finds the next available scanning machine by iteratively performing a test **204** to determine if the scanning machine designated as the current value of the iteration variable is available and, if it is not available, incrementing **206** the iteration variable and returning the thread of execution to test **204**. When a scanning machine is found to be available, the necessary scan related information is copied **208** from the central computer **120** to the scanning machine and a message is e-mailed **210** to the user that indicates that a scan is scheduled and that the scan is commencing. The central computer **120** then instructs **220** the scanning system to establish communication with the remote computer system via a global computer network and commence the scan.

Once the scanning machine begins performing the scan, the central computer **120** repeatedly performs a test **212** to determine whether a "scan complete" indication is received from the scanning machine. If a "scan complete" indication is received, then an e-mail is sent to the user **214** indicating that the scan is complete. The results of the scan are then recorded **216** in a database resident in the central computer **120** or on a file system of another database machine. The results could include an indication that the scan is complete, the date and time of the scan, the nature of the tests performed during the scan and the nature of any deficiencies detected by the scan. The results of the scan may then be used for generating a scan report and other uses, such as statistical analyses, *etc.*

While one illustrative embodiment of the procedure executed by the central computer **120** is shown in FIG. 2, it will be readily understood that many other scan scheduling algorithms could be employed without departing from the scope of the invention so long as the algorithm employed provides for scheduling a scan of a remote system, selecting an available scanning machine and instructing the selected scanning machine to execute a scan via a global computer network.

The above described embodiments are given as illustrative examples only. It will be readily appreciated that many deviations may be made from the specific embodiments disclosed in this specification without departing from the invention. Accordingly, the scope of the invention is to be determined by the claims below rather than being limited to the specifically described embodiments above.